DOCUMENT RESUME

ED 442 815 TM 031 235

AUTHOR	Rosen, Gerald A.
TITLE	Computer-Based Testing: Test Site Security.
PUB DATE	2000-04-00
NOTE	8p.; Paper presented at the Annual Meeting of the National Council on Measurement in Education New (Orleans, LA, April 25-27, 2000).
PUB TYPE	Opinion Papers (120) -- Reports - Descriptive (141) -- Speeches/Meeting Papers (150)
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	Adaptive Testing; *Computer Assisted Testing; *Testing Problems
IDENTIFIERS	*Test Security

ABSTRACT

Computer-based testing places great burdens on all involved parties to ensure test security. A task analysis of test site security might identify the areas of protecting the test, protecting the data, and protecting the environment as essential issues in test security. Protecting the test involves transmission of the examinations, identifying the examinee, and supervising test administration. Protecting the data means ensuring that it does not fall into the wrong hands, while protecting the environment involves many considerations on the part of test administrators. Simplifying the jobs of test administrators may eventually result in tests administered over the Internet, with tests and data residing at the Web site. Such a system might enhance security and simplicity. Three appendixes discuss the role of appointment scheduling software in the protection of the examination, provide an example of a test site data protection system, and contain an example of a system designed for disaster recovery at a central data center. (SLD)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 442 815

Computer-Based Testing: Test Site Security

Gerald A. Rosen, Ed.D

Executive Consultant

Prometric

G. Rosen

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
☑ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

The term "security" as applied to high-stakes computer-based testing test sites refers to many different things most of which have a direct analog in paper-and-pencil testing. In both situations, examinees must be identified, examination administrations must be supervised and proctored, and the security of examinations and data must be assured. However, it is my observation that in computer-based testing (CBT) the overall process is much more complicated and places greater burdens on all involved parties - from measurement professionals to hardware and software experts to onsite test administrators.

CBT is a technology intensive medium. Technology is used to deal with the complexities of security issues and problems both at local test sites and at central data centers. Later on in this paper I will discuss some of the current limitations of technology in dealing with test site security issues and how changes in technology that are just beginning to receive wider application may hold the key to dramatically reducing the security burdens at the test site.

A task analysis of test site security might come up with the following broad areas: (1) Protecting the test; (2) Protecting the data; and (3) Protecting the environment. The first two of these areas have the most obvious connections to test site security.

1. Protecting the test

Protecting the test in a CBT context has much the same meaning as it does in paper-and-pencil testing. In other words, the test has to reach the test site, be safeguarded while there, administered correctly to the appropriate persons, and safely returned.

1.a) Transmission of examinations - Protecting the test begins with getting it securely to the test site and back. This may involve communication via telephone lines, high-speed ISDN telephone lines, the Internet, or computer-readable media, such as diskettes, sent via a secure carrier like Brinks or an overnight shipper like UPS. Communications are usually encrypted, with decoding occurring only at the time of the actual presentation of items to the examinee. Encryption is the main security tool for protecting the test both during its transmissions to and from the test site and also while there. It also represents a major advantage over paper-and-pencil testing, where encryption is not a realistic possibility.

TM031235

BEST COPY AVAILABLE

In some CBT systems, the test remains at the test site only for a brief period of time and is returned after the examinee's appointment. In others, examinations reside at the test site during the entire period of time that they are available for use. In either case, physical security mechanisms (i.e., locks, burglar alarms, bolting equipment to the floor, etc.) are used to discourage or prevent theft of equipment containing the encrypted examinations and examination data (i.e., examinee responses to items, examination results, etc.). Software security mechanisms are used to help ensure that only eligible individuals gain access to examinations. Often this aspect of security is controlled by appointment scheduling software which only allows eligible examinees to make appointments and also prohibits the on-site delivery of an examination in the absence of a valid appointment. Other software security mechanisms prevent on-site staff from printing copies of examinations or otherwise gaining access to examinations for purposes other than test administration (Appendix A contains a brief example of scheduling software control of appointments and test delivery.)

1.b) Identifying the examinee - Another major component of protecting the test is ensuring that the right person takes the test. In most CBT testing programs, just as in most paper-and-pencil programs, the acceptable mode of identification remains two forms of identification, one government issued and with a picture, and another with a signature or photograph. In other programs, additional documentation must be brought to the test site. These documents might include admission tickets, authorization to test letters, professional or occupational credentials, etc. Examinees must sign in, and possibly sign out, in a register, log book, or daily test roster. Some higher stakes programs, usually licensure programs, may also require that a picture be taken with a digital camera so that the image can be stored on computer and transmitted back to the sponsoring agency along with the test results. A few testing programs require finger or thumb printing. This process is still mostly manual, but there are now proprietary digital systems, such as *Identix*, that can take up to ten prints and store their images in a computer file. Other forms of biometric identification systems, such as retina or iris scan, can be used in conjunction with computer-based testing. Chances are that we will soon see an increase in the use of biometric identification, but the possibility of examinee backlash should not be overlooked. In at least one certification program that I am aware of, complaints against the intrusiveness of picture taking are an almost daily occurrence. Given this fact, it is possible that a significant number of refusals to submit to fingerprinting and, possibly, to retina scan will occur and may lead to a more than trivial drop in numbers tested on non-required examinations.

1.c) Supervising the test administration - When we administer examinations, at some point in this increasingly complex process we find ourselves faced with a room full of people taking tests. Whether paper-and-pencil or CBT, it remains a good idea for someone to watch them do it. At least for now, CBT is usually executed in permanent locations. This affords the opportunity to use observational technology not readily available in temporary or ad hoc venues. This includes videotaping, audio monitoring, audio taping, observation windows, and parabolic mirrors. None of these should be seen as entirely replacing proctoring by test site staff. Indeed, the observation windows and parabolic mirrors are intended to aid direct proctor observation. As always, the enhanced technology on-site serves as an additional deterrent to activities like cheating and the

clandestine copying of examination items. However, it would be a mistake to assume that the technology reaches the level of prevention. For example, with respect to video taping, it is reasonable to assume that knowing that they are being taped, examinees will be less likely to cheat. Those who do, and whose activities are captured on tape, are still likely to escape detection unless directly observed. This is the case because tapes are not routinely reviewed unless a direct observation of suspicious behavior has been made.

2. Protecting the data

Protecting the data means more than ensuring that it doesn't fall into the wrong hands. It also means ensuring that the data find the way back to their owners in complete or uncorrupted form. Threats to the integrity of the data and its successful routing to testing program sponsors (or their testing companies or consultants) can come from a variety of sources. Some of these include power outages, data transmission problems, and catastrophic software or equipment failures at test sites or centrally located data centers. In these instances, the key to successful data protection lies in data backup and system redundancy.

Appendix B contains a brief description of the hardware and software-based data protection system used by Prometric in its STC network of high-stakes testing centers.

Although somewhat outside the scope of this paper, Appendix C contains a brief description of the hardware and software-based data protection system used at the Prometric central data center.

3. The primary test-site security issue

No matter how much hardware and software control is exercised over the testing process, security ultimately resides in the hands of the test center staff. They are the ones who (1) determine who actually gets to sit at a computer to take a test; (2) ensure that security procedures are followed; and (3) are charged with making certain that examinees don't cheat or copy test items. Wall-mounted cameras are of no use if monitors at the test administration station are ignored. Video tapes made on machines that have not been cleaned or even turned on are useless. Carefully counting and distributing sheets of scratch paper is an ineffective means of keeping examinees from copying items when nobody bothers to collect them at the end of an examination.

At a typical paper-and-pencil test site, staff are most often responsible for administering one or several examinations produced by a single sponsor. Just about everything the test administrator needs to know is contained in the proctors' manual. Everyone starts the test at the same time. The examination(s) last from a few hours to a full day, after which the test materials are packed up and everyone goes home.

At a CBT site, examinations are administered six days per week to examinees taking any one of hundreds of tests provided by dozens of sponsors, at the very least. There is a great deal to know to do the job correctly. Although hard-copy and online proctors' manuals are available, the sheer amount of information makes mastery difficult. In addition, throughout the day some examinees are beginning examinations while others and completing theirs. Still others may be calling on the telephone for directions to the center or to cancel or reschedule appointments. If you've never been to a busy CBT center, you might be surprised to discover just how busy it is and how much it resembles a hotel reception desk operating at peak check-in and check-out times. CBT test center administrator is a tough job - and it doesn't pay very well.

In my opinion the best way to ensure a secure, high-quality test administration is to simplify the job of the test administrator. The most complicating factors for the test administrator are the tests themselves, and all of the hardware, software, and security procedures required for their protection and for the protection of the data generated by the testing process. Thus, it follows that the best way to ensure security at the CBT test site is to get rid of the tests and the test-related data. It may sound like an odd proposal, but it really is not hard to do. Test centers can be nothing more than rooms with computers and high-speed Internet connections. Examinees would rent seat time at workstations, log on to a Web site, type in an authorization number and take their tests. Tests would reside at the Web site as would all the test results data. Examinees would receive their scores on-screen, and/or via email, and/or through the mail.

In this system, the CBT test site would look virtually identical to the way it does today. It would still consist of a testing room with desks and computers. In reality, however, it would be nothing more than a proctored location for test taking. It would be similar to the CBT test centers of today, but with the network ripped out and replaced by high speed links to the Internet. The Test Center Administrator would remain responsible for verifying identification and, most importantly, watching people take tests. While there would still be a certain amount of information unique to some testing programs, test administrator prompt screens at the Web site could be used to remind proctors which tests permit the use of scratch paper, calculators, etc.

If a digital photograph of the candidate is required, it can be taken by a relatively inexpensive computer-mounted camera. Similarly, the gathering of other candidate biometric data collection can be collected in automated fashion and without the intervention of the proctor. In this simplified testing center, all of the aids to proctoring and the observation of test behaviors would remain in place. Audio and video taping and monitoring, parabolic mirrors, and observation windows would remain part of the standard CBT test center equipment.

Test centers operating in this fashion would not need to be linked to a central data center or to each other. This would further enhance security and simplicity. The only external computer linkage might be to a reservations system similar to the ones now in use by hotel chains. Such a reservations system would further unburden test center staff by freeing them from the responsibility for examination scheduling and from receiving routine calls for information, such as driving directions to the center, center hours of operation, etc. All basic information about the

test centers would be located within the reservations system. It might even be realistic to make the reservations system fully Internet based, thus eliminating the need for, and enormous expense of, a fully staffed, centralized call center.

In short, a system of free-standing, proctored locations where examinees can gain access to CBT examinations will enhance security by reducing the information burden on proctors and the number of tasks they are required to perform. This will leave them in a position to spend more time identifying examinees and proctoring. It is likely that it will also significantly reduce test site costs and return control of and responsibility for examinations back to testing program sponsors.

In closing, I would like to add that I recognize that removing examinations and examination related data from the computerized test sites does not resolve the security problems and issues for tests and test data. It moves them somewhere else: namely to the entities that will host examinations on the Worldwide Web portion of the Internet. For the Web hosts, the same security issues will remain and others, such as security of Internet transmissions, may be introduced. However, I maintain that for the reasons cited above, security will be enhanced by moving tests out of the testing centers.

Furthermore, I maintain that there will be another important benefit. Examinees and testing program sponsors hold CBT vendors to a standard unheard of in paper-and-pencil testing. Examinees complain bitterly about conditions that they would have died for when almost all tests were paper-and-pencil. Failing examinees routinely demand free re-tests for such reasons as: 1) The test started 15 minutes late causing my anxiety to become uncontrollable; 2) I was unable to concentrate because of the distraction caused by assistance given to other examinees; 3) The driving directions to the test center failed to take note of a construction zone and I became upset by this terrible lack of sensitivity, etc. (All of these true.) Indeed, testing program sponsors who formerly told examinees with similar complaints, either politely or not so politely, to "take a hike" when they were responsible for their own paper-and-pencil sites, now regularly become vociferous advocates for examinees with even bizarre complaints when a commercial CBT vendor is involved.

Despite the often unreasonable demands of examinees and sponsors, does anyone have the right to say that a higher standard, although not an irrational one, isn't justified? After all, the fact is that there is usually much more money to be made by simply administering an examination via CBT then there is in designing, developing, and ensuring the quality and validity of the same examination. The world's largest CBT vendor was recently sold for more than three-quarters of a billion dollars. That price would not have been paid if the company weren't making hundreds of millions of dollars each year. With that kind of money in the equation, I contend that a higher level of service to both the examinee and the sponsor should be expected and delivered.

Such expectations of quality, as well as examination security, will never be met until the job of the test administrator is simplified and brought into some kind of reasonable balance with these

expectations. Technology has a way of changing one's perspective on a pretty frequent basis. However, for the time being, at least, I see the much of the solution to the problem of examination security and test administration quality resting with the separation of test site and test.

Appendix A - An example of appointment scheduling software control in the protection of the examination.

Prometric's professional licensure and certification programs are "eligibility-based", meaning that examinations are available for administration only to individuals who have been designated as eligible by examination program sponsors. Electronically transmitted eligibility lists serve as the established method of eligibility information transfer. Once an eligibility record has been received, it is imported directly into the scheduling system and creates the registration record used to track the examination process. This record contains information regarding the examinee, the program, the test within the program to be taken, and the eligibility period. Without this record, the examinee will not be able to schedule an examination.

The Prometric scheduling software permits only one testing appointment per eligibility record. Once an appointment is made there are only three options: (1) cancel the appointment; (2) change the appointment (which automatically cancels the previous appointment); or (3) take the test at the place and time scheduled. Once a test is started, the eligibility record is deleted from the scheduling database, thereby prohibiting the examinee from scheduling another appointment.

At the test center, software control is maintained via the "Administration Station" (i.e., the test administrator's computer). Pre-installed software specifies the functions that can be performed and, in so doing, prohibits all others. For example, the test administrator can perform the start-of-day function to open the test center, inform the scheduling system that an examinee has arrived, initiate the process of test administration to an examinee, and move the test administration to another workstation in the event of a technical problem. On the other hand, there is no test print function and no function that would permit the delivery of a test in the absence of a scheduled appointment.

Appendix B - An example of a hardware and software-based test site data protection system

Each Prometric STC testing center automatically runs a virus detection program as part of the start of day procedures. For enhanced reliability, the communications network uses ISDN lines to communicate with the STCs. To minimize the potential consequences of catastrophic failures, testing centers are queried every two hours by the central data center for examination information. This is a fully automated process. Thus, examination results are moved to the central data center

both during test sessions and, finally, at the first communication after examinations have ended. This occurs no later than two hours after completion of an examination.

While an examination is being delivered to an examinee, a record for each response is written to the hard disk. If a power failure occurs, examinees can restart at the same point in the examination where they were working at the time of the disruption. All previously captured information is retained. An uninterrupted power supply (UPS) at each center ensures that no data are lost when a power outage occurs.

The examination result file contains all examination-related data, including scoring information, the response string, response latencies, etc. When an examination is completed, three copies of the examination result file are created. The first copy is placed in the communications queue, from which it is moved to the central data center on the next "two-hour" communication. After the communication is successfully completed, it is deleted from the queue. The second copy is placed in a communications backup system. This is a rotating backup from which it is automatically deleted after thirty days. The third copy of the examination test result, the original file that was created as the examinee took the test, is saved for a period of three (3) months at the test site.

Appendix C - An example of a system designed for disaster recovery at a central data center.

At Prometric world headquarters in Baltimore, all data maintained at the central data center are stored in multiple locations to ensure data recovery. All database servers utilize a mirrored storage system, where the data is simultaneously written to two hard drives. The central data center file server also provides System Fault Tolerance Level III, which requires a mirrored server. All database transactions are simultaneously logged to an alternate server.

The central data center uses two levels of backup. First, the system is completely backed up on a daily basis to tape. These tapes are never rotated, and are stored off-site. Second, all results data are copied onto optical disk daily, ensuring a convenient, timely on-site recovery method.

The central data center itself is replicated in an alternate location five miles distant. The alternate data center is complete with redundant hardware and communications to allow a quick recovery in the event of large-scale disasters.

All systems at the central data center employ continuous detection virus detection software. All remote network gateways are fully segmented from accessing the Data Center network.